Cloud computing

Livre blanc rédigé par le Groupe *Cloud Computing* de l'ADIRA

Introduction : le Cloud, pour quoi faire ?

Pierre est le DSI d'une PME qui œuvre dans le domaine de l'industrie. Tous les trois ans, cette entreprise a choisi de renouveler l'infrastructure serveurs et stockage de son système d'information et l'heure est venue pour Pierre de présenter une nouvelle étude sur ce renouvellement.

… Et c'est aujourd'hui que Pierre commence à se « prendre la tête » pour ébaucher ce que sera la nouvelle plateforme informatique de son entreprise pour les années à venir.
Tous les trois ans, Pierre a la désagréable impression de partir d'une feuille blanche. Bien que le prix des matériels soit depuis des années à la baisse, il a de plus en plus de mal à expliquer à sa hiérarchie que tous les trois ans, il faut « jeter » les anciens équipements pour en racheter de nouveaux (en espérant qu'ils dureront au moins aussi longtemps que les précédents !).

L'activité industrielle de son entreprise est sujette à des pics bisannuels qui demandent pour ces moments-là des ressources supplémentaires en puissance et stockage.
Il lui faut donc tous les trois ans réussir le tour de force de présenter un budget d'investissement (annuel) dans lequel est provisionné une infrastructure dimensionnée pour dans 3 ou 4 ans … en période haute !

A chaque fois les mêmes questions le taraudent :

- L'infrastructure est-elle bien dimensionnée pour la période ? ni trop, ni trop peu.
- Si une embellie économique survient, supportera t'elle la charge jusqu'au bout ?
- A contrario si l'entreprise subit une crise, comment vais-je pouvoir utiliser la puissance en trop ?
- Comment expliquer dans mon argumentaire que l'on achète de la puissance et du stockage maintenant … pour dans trois ans ?
- Si cette puissance et ce stockage ne suffisent pas en fin de période, comment vais-je expliquer ce surplus d'investissement pour une plateforme qui nous coûte déjà cher ?
- Mon effectif est-il suffisant pour à la fois mener les projets nécessaires au développement de l'entreprise et l'administration d'une plateforme informatique ?
- Comment gérer la complexité des divers contrats de maintenance ?

… et ainsi les nuits se succèdent … on réfléchit mieux la nuit !!!

Un beau matin, alors que le soleil brillait dans un ciel … sans nuage, la presse informatique que lisait Pierre parlait, elle… de nuages !

Un nuage qui, après approfondissement, semblait apporter un certain nombre de solutions à notre DSI.

D'abord il lui semblait comprendre qu'il ne s'agissait pas d'acquérir du matériel mais plutôt du logiciels sous forme de services (lorsqu'il s'agissait d'applications) et sous forme de machines virtuelles (lorsqu'il s'agissait de Systèmes complets).

De plus les messages diffusés dans la presse par les nouveaux fournisseurs de ces nouvelles offres indiquaient qu'il s'agissait de facturer à l'usage et que les dimensions de ces offres pouvaient varier en fonction des besoins de l'entreprise et cela très rapidement à la hausse comme à la baisse. En quelques minutes.

… La mariée était très belle !...

Cependant après plusieurs jours d'investigations, Pierre dû se rendre à l'évidence, la mariée était TROP belle. En effet non seulement les offres étaient techniquement loin d'offrir (encore) autant de souplesse qu'elles le présentaient, mais tous les systèmes d'exploitation n'étaient pas encore proposés et un certain nombre de questions se posaient tant sur le plan financier que sécurité et légalité.

Pierre choisit donc la prudence et décida de chercher pour quels autres projets de l'entreprise les promesses du Cloud seraient plus susceptibles de se concrétiser: Accessibilité des applications, fiabilité des réseaux, mise à jour des logiciels sans rupture de service, passage d'une logique d'immobilisation à une simple charge d'exploitation …

Tout en se promettant d'essayer de lancer rapidement un premier pilote.

Ce qu'il faut retenir :

Après s'être enthousiasmé pour le Cloud à la lecture de la presse, Pierre se rend compte que, comme toute nouveauté informatique, le Cloud ne tient pas toutes ses promesses lorsqu'on le confronte à la réalité des exigences d'un projet concret.

Prudent, il décide de mieux identifier les opportunités apportées par le Cloud.

Il choisit de participer, dans le cadre de son adhésion à l'Adira, au Club Cloud Computing, afin de mieux discerner grâce à ce groupe d'échange les avantages, inconvénients et bonnes pratiques du Cloud, pour pouvoir tirer le meilleur parti de cette technologie… pour ses futurs projets.

Définitions, terminologie

Qu'est-ce que le « cloud » ?

Selon une définition donnée par le NIST (US National Institute of Standards and Technology), le « cloud computing » est un modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressources informatiques (par exemple des serveurs, des espaces de stockage, des applications) qui peuvent être rapidement mises en service avec un effort minimum de gestion et d'interaction avec le fournisseur de ce service.

Ce modèle favorise la disponibilité, il est défini par cinq caractéristiques essentielles, trois modèles de service et quatre modèles de déploiement.

Caractéristiques

1. Self-service, à la demande : capacité à fournir une ressource informatique automatiquement, sans requérir d'interaction humaine côté fournisseur
2. Accès réseau : ces ressources sont accessibles au travers d'un réseau, par des protocoles standards
3. Ressources partagées, mises en commun : capacité à fournir dynamiquement des ressources selon la demande de l'utilisateur, prises dans un pool commun
4. Élasticité : possibilité de faire évoluer très rapidement la capacité fournie, que ce soit en plus ou en moins
5. Mesurable : capacité à mesurer le service fourni. L'utilisation des ressources peut être surveillée, contrôlée et signalée, offrant la transparence pour le fournisseur et le consommateur du service utilisé. Cette caractéristique permet en particulier de payer le service à l'usage.

Modèles de service

On distingue trois modèles différents, selon ce qui est délivré par le fournisseur :

1. IaaS : Infrastructure as a Service. Exemple : fournir de l'espace de stockage
2. PaaS : Platform as a Service. Exemple: fournir un serveur Windows sur lequel il ne reste au client qu'à installer son application
3. SaaS : Software as a Service. Exemple: fournir une application de messagerie









Géré par le département IT interne

Géré par le fournisseur du "cloud"

Modèles de déploiement *cloud* public / *cloud* privé

1**) Cloud privé :** caractérise une infrastructure cloud qui est propriété d'une seule entreprise et n'est utilisée que par elle. Cette infrastructure est toutefois intégralement possédée et gérée par un opérateur Cloud externe.

2) **Cloud public :** caractérise une infrastructure cloud qui est accessible et mutualisée entre tous les utilisateurs.

> Note : il existe deux autres modèles, « 3) communautaire » et « 4)hybride » qui caractérisent respectivement des clouds partagés par une même communauté –universitaire par exemple– et des clouds composés de deux ou plus des modèles précédents ; mais ils sont aujourd'hui peu répandus.

Ce qu'il faut retenir :

Ne pas confondre cloud et hébergement : ce dernier consiste à louer un espace dans un datacenter pour y installer ses propres ressources informatiques, dédiées, dont on conserve tout ou partie du contrôle (maintenance, évolution, etc.).

En utilisant des ressources cloud, on n'est pas propriétaire des ressources, ni en charge de leurs capacités ni de leurs maintenances, ni de leurs évolutions, etc.

Ceci confère au Cloud l'un de ses avantages essentiels qui est de pouvoir se consacrer pleinement à la problématique métiers sans souci d'infrastructures.

Force, Faiblesse, Opportunité, Menace du Cloud Computing dans le SI

Les diagrammes SWOT ci-après, élaboré lors d'une réunion de travail, sont proposés par le Club pour aider le DSI dans son analyse d'opportunités.

Organisation et gouvernance

	FORCES	*FAIBLESSES*
INTERNE	**❖ Indépendance des ressources internes (24/7)** **❖ Facilite les projets de mutualisation, regroupement de structures (solution qui arbitre les solutions déjà existantes)** **❖ Facilite le nomadisme et le télétravail** **❖ Gain sur les coûts de prestations** **❖Gain sur les délais** **❖Favorise l'innovation, débloque certains projets car pas besoin de dimensionner des serveurs** **❖Possibilité de se conformer à des obligations légales de gouvernance et de sécurité à moindre coûts** **❖ Pas d'investissement dans l'infrastructure**	**❖ Conduite du changement impliqué par les mises en ligne de nouvelles versions obligatoires** **❖ Nécessité d'une très bonne définition des Slas dans les contrats (pas toujours évidente à formaliser)** **❖ Peut complexifier PRA/PCA par la multiplication des sites d'hébergements** **❖ Nécessite de se doter de nouveaux outils de contrôle de performances pour maitriser la qualité**
	OPPORTUNITES	*MENACES*
EXTERNE	**❖ Correspond à une évolution des DSI vers plus de maitrise métier et moins d'exploitation et déploiement d'infrastructures** **❖ Obligation pour les prestataires de se conformer à des normes (par exemple ISAE 3402)**	**❖Risque de perte des compétences internes nécessaires pour assurer les choix, les migrations et le contrôle qualité**

Logiciels

	FORCES	*FAIBLESSES*
INTERNE	**❖Facturation à l'usage** **❖ Mise à jour automatique intégrée au contrat** **❖Evolutivité plus rapide des licences et des droits, intégrée au contrat** **❖ Mise en œuvre plus rapide** **❖ Moins de coûts de mise en oeuvre** **❖Solution cloud très adaptée a l'usage ponctuel, périodique, temporaire, innovant, nouveaux projets**	**❖ Complexification de l'urbanisation du SI** **❖ Manque d'adaptabilité aux besoins spécifiques et au « sur mesure » (niveau fonctionnel),** **❖L'utilisateur doit s'adapter aux services catalogues** **❖ Difficulté d'intégration au sein des architectures existantes, peut complexifier l'authentification**
	OPPORTUNITES	*MENACES*
EXTERNE	**❖Très fort développement de l'offre « Saas », permettant de disposer d'une offre de plus en plus large** **❖ Réduction du coût total de déploiement des nouvelles solutions** **❖Réponse aux besoins de mutualisation, fusion, groupement de commandes…**	**❖ Réversibilité (manque de standard)** **❖ Perte de maitrise du SI par l'entreprise par des usages cloud à l'initiative des utilisateurs et sans contrôle par la DSI** **❖ Risque de revenir à une informatique en silos, avec un manque de transversalité (urbanisation)**



Données

	FORCES	FAIBLESSES
INTERNE	❖ Meilleure résilience des données dans le cloud ❖ Plus d'effet de seuil (volume de données) ❖ Facturation performante à l'usage de l'espace consommé ❖	❖ Non maitrise de la localisation des données ❖ Complexification de l'archivage ❖ Risque de ne plus respecter les directives légales d'archivage ❖ Renforce les exigences en terme d'archivage / restauration ❖ Manque de maitrise de la confidentialité des données
	OPPORTUNITES	MENACES
EXTERNE	❖ Très adapté aux projets pilotes, aux essais, à l'innovation ❖ Offre de stockage dans le cloud très compétitive ❖ Forte capacité d'adaptation aux demandes	❖ Réversibilité (manque de standard) : restitution des données fin de contrat, peuplement initial de la base en début de contrat ❖ Interopérabilité (échange entre solutions) ❖ Responsabilité en cas de perte de données ❖ Perte de maitrise du SI par des usages cloud à l'initiative des utilisateurs et sans contrôle ❖ Localisation géographique des données (CNIL) ❖ Risque de suppressions automatiques des données ❖ Facturation automatique en fonction des volumes, non maitrisée ❖Augmentation du risque liée à la concentration des données

Infrastructure technique

	FORCES	FAIBLESSES
INTERNE	❖Puissance et capacité évolutive de façon « instantanée » ❖ Délais de mise en œuvre très réduits ❖ Facturation a l'usage ❖ Suppression des effets de seuils (serveurs) ❖ Favorise l'indépendance vis-à-vis du terminal utilisateur ❖ Optimise l'usage des ressources ❖ Fait disparaitre le problème d'adaptation du datacenter ❖ Facilite la mise à disposition 24/7	❖ Perte de maitrise des architectures ❖ Perte de visibilité sur l'infrastructure (supervision), ❖Complexification de la sécurité ❖ Augmentation des contraintes réseaux et Internet ❖ Peu adapté pour les zones géographiques où l'offre haut débit opérateurs est faible ❖Multiplication des extranet d'administration
	OPPORTUNITES	MENACES
EXTERNE	❖ Offres encore jeunes appelées à murir ❖ Solution Cloud peut être complémentaire des infrastructures existantes et non en opposition ❖ Peut faciliter la démarche « bring your own device » ❖Coût très performants pour des démarrages d'activités	❖En cas d'attaque Internet ou de déni de service, perte de production (plus d'informatique locale) ❖ En cas de mauvaise performance, le diagnostic et la preuve de la localisation de la défaillance peuvent être très complexes ❖Offre catalogue pouvant ne pas répondre à toutes les demandes spécifiques

Proposition d'une cartographie des applications éligibles au Cloud Computing (quelle sont les meilleures applications à migrer ?)

La cartographie ci-après, élaboré lors d'une réunion de travail, est proposé par le Club pour aider le DSI à prioriser ses projets Cloud Computing.

Les « ++ » signalent que la solution Cloud Computing est potentiellement une bonne alternative à une solution traditionnelle pour le domaine technique ou fonctionnel listé.

Les »--« indique qu'il convient d'être vigilant vis-à-vis du domaine technique ou fonctionnel listé si on envisage une approche Cloud Computing

Contrainte vrai pour tous les cas : disponibilité du réseau

Domaine technique ou fonctionnel	Intégration au SI (++ simple --difficile)	Réversibilité (++ simple -- difficile)	Risque sur la confidentialité des données (++ faible -- forte)	Maturité des offres (++ forte -- faible)	ROI (++ Rapide -- lent)	Contraintes	USAGES CLASSIQUES
Infrastructure (IAAS)							
Espace stockage données	++	++	--	++	++	**Dimensionnement réseau**	Sauvegarde Serveurs de fichiers
Serveurs virtuels (CPU) – DEV	++	++	NA	+	+		Environnement test/dév/QA
Serveurs virtuel (CPU) - PROD	+	+	--	+	+	**Supervision contrôle des coûts**	Besoin de calcul Evénementiel Reporting
Systèmes (PAAS)							
Hébergements WEB	++	++	--	++	++		Sites web, plateformes marchandes…
Serveurs d'applications (runtime : exemple Java, PHP, Forces.com, Azure, GoogleApps)	-	--	+	++	++	**Attention aux caractères « propriétaire » des environnement / existe il une version on premise ?**	Applications spécifiques
Intégration SOA (Run My process, …) (Intégration Cloud ou hybride)	++	--	-	-	++	**Attention aux caractères « propriétaire » des environnement / existe il une version on premise ? Chiffrement des données**	ETL, EAI, BPM, BPO

Logiciels pré-packagés (SAAS)							
	Intégration au SI (++ simple --difficile)	**Réversibilité (++ simple -- difficile)**	**Risque sur la confidentialité des données (++ faible -- forte)**	**Maturité des offres (++ forte -- faible)**	**ROI (++ Rapide -- lent)**	**Contraintes**	**USAGES CLASSIQUES**
ERP (SAP Business by design), **Paye, RH (Cegid, Sage, …)**	-	--	--	--	--	Attention à la disponibilité des connecteurs / Limite dans la personnalisation vis-à-vis on-premise	Très récent
Business Intelligence (Ex : Bittel,)	++	+	--	+	++	Attention à la disponibilité des connecteurs / Limite dans la personnalisation vis-à-vis version on-premise / souplesse peuplement des données	
CRM (ex : Dynamics, Force.com)	++	+	-	++	++		
Bureautique collaborative (Office365, Googleapps) **(Sharepoint, Vdoc…)**	++	++	-	++	++	Complétude et richesse fonctionnelle / Attention fonctionnalités mode hors connexion	Usage standard / Collaboratif
Messagerie, antivirus, antispam	+	++	-	++	++	Attention à l'intégration communication unifiées	
Project management	++	+	-	++	++		Planification collaborative et multi sociétés
Conférences web (Webex, …)	++	++	++	++	++		
Sauvegarde du poste de travail (Dropbox, …)	++	++	--	++	++		Disque dur virtuel
Communications unifiées (Lync, Skype, Google Apps,...) Centrex IP	-	++	--	++	++	Attention intégration à la téléphonie d'entreprise / maitrise de l'enregistrement des conversations	

Ce qu'il faut retenir :

On peut imaginer couvrir l'ensemble des besoins informatiques d'une organisation par des solutions Cloud, mais cela sera rarement pertinent.

Par contre, le Cloud Computing présente une complémentarité très intéressante vis-à-vis des solutions traditionnelles dans certains contextes ou sur des domaines précis.

Le Cloud Computing permet d'essayer plus facilement des approches innovantes, sans se préoccuper des problèmes d'infrastructures ou de montées en charges, ni des investissements associés. Il est pertinent pour les usages périodiques, événementiels. Il peut faciliter la mise en place de projets communs entre des entités différentes, en évitant les « querelles de clochers ». Il répond à des exigences de disponibilités fortes 24/7 pour lesquels les équipes et les data center existants ne sont parfois pas organisées.

Le Cloud Computing tire son épingle du jeu pour les machines de développements, les plateformes d'hébergement et de conception de sites web, la bureautique, la messagerie, certaines briques de communication unifiées, le CRM et les espaces de collaboration.

Cas typiques d'utilisation

Sur le plan de la Production :
- Un dimensionnement qui suit au plus près les besoins en fonction des périodes hautes et basses
- Une réactivité de mise ne production (quelques heures à quelques minutes)
- des mises à jour « On Line » sans interruption du service.
- Une sécurité et une disponibilité proche des 100%
- …

Sur le plan des Développements :
- Utilisation de machine virtuelles à l'usage permettant de réaliser des tests ponctuels sur les nouvelles applications avant mise en production ou d'effectuer du débogage ponctuel en reproduisant à la demande un environnement de production sans interrompre ce dernier.

- Capacité à sur-dimensionner la plate-forme utilisée pour permettre d'effectuer des tests de charges censés représenter la situation dans plusieurs années
- Réactivité dans la mise à disposition des environnements (quelques heures à quelques minutes)

… plus globalement :

- Paiement à l'usage,
- Les équipes du SI se recentrent sur les projets métiers,
- Suppression (ou diminution) de la gestion des contrats de maintenance,
- Financièrement les solutions migrées sur le Cloud deviennent une simple charge d'exploitation.

Ce qu'il faut retenir…

Les différences notoires entre un système d'information traditionnel et une solution de Cloud computing, reposent principalement sur 3 caractéristiques :
- Un service à la demande (il s'agit toutefois essentiellement d'une solution catalogue, les possibilités d'adaptations aux besoins spécifiques étant réduites)
- Une agilité dans la mise en œuvre
- Le paiement à l'usage.

Impacts techniques du cloud sur le SI de l'entreprise

Impacts sur les applications.

En général

Dans tous les modes, le client de la solution *cloud* doit suivre l'évolution de l'implantation de la solution : niveau de version du *cloud*, API d'accès au *cloud*, mode d'emploi vu par les utilisateurs. C'est une des caractéristiques du cloud : vous ne vous occupez pas de la plateforme d'accueil de votre informatique ; elle évolue toute seule ; les mises à jour sont réalisées par le prestataire !

Aujourd'hui, les produits logiciels diffusés de façon classique voient naître une version majeure tous les 3 ou 4 ans ; les solutions de type *cloud* devraient voir cette fréquence largement s'accélérer, à un rythme d'une version majeure tous les 6 à 18 mois.

À titre d'illustration, un certain nombre d'entreprises utilisent encore Office 2003 aujourd'hui. Un tel « conservatisme » ne sera plus autorisé par le Cloud Computing, ce qui présente certains avantages, mais aussi des inconvénients et des coûts non négligeables de conduite du changement, pour une valeur ajoutée parfois discutable.

En mode SaaS

Qu'en est-il de l'interopérabilité entre logiciels ou progiciels implantés dans le *cloud* et ceux qui sont intégrés dans les serveurs de l'entreprise ?

La plupart du temps, les éditeurs de solutions en mode SaaS proposent des connecteurs pour les principales solutions du marché et pour les formats de données standard. En dehors de certains cas spécifiques, ces connecteurs s'avèrent en général suffisants pour répondre aux besoins d'intégration.

Dans le cas contraire, des acteurs du *cloud computing* proposent des connecteurs dédiés ou des process (application « Run My Process », par exemple).

Les connecteurs dédiés (Salesforce.com, Google Apps, outils Microsoft en ligne tels que Office365 ou CRM Dynamics, ...) permettent de contrôler l'accès à ces applications. Il suffit généralement d'activer une option dans le panneau d'administration de l'application.

L'idée reçue : le mode SaaS repose sur une mutualisation des ressources et des applications qui doivent s'adapter au plus grand nombre, il est donc impossible de faire du spécifique. Il peut en résulter un intérêt très relatif pour le SaaS par rapport à des développements internes ou des solutions *on-premise*.

La réalité : les solutions proposées en mode SaaS sont des progiciels comme les autres. Seul le modèle de déploiement et d'usage diffère : comme toutes bonnes solutions, elles sont paramétrables afin de s'adapter aux différents clients. Certains éditeurs d'offres SaaS vont même jusqu'à ouvrir leur plate-forme à des partenaires à travers des interfaces de programmation (API) pour leur permettre de développer et de proposer extensions et modules complémentaires.

En mode PaaS

L'offre en mode Paas, est aujourd'hui limitée : Amazon, Microsoft Windows Azure, Google App Engine. Chacune des plateformes est spécifique, même pour Windows Azure, dont le nom pourrait laisser supposer qu'il s'agit d'une plateforme Windows, alors qu'il faut plutôt considérer cette plateforme comme un environnement d'implantation d'application .Net.

La conséquence de cette spécificité de chaque plateforme est de devoir adapter spécifiquement les applications à la plateforme PaaS installée dans le *cloud*.

Impacts causés par la plateforme

La plateforme utilisée par le fournisseur de service Cloud ne devrait pas être la préoccupation du client puisqu'elle concerne l'intérieur du *cloud*. Cependant il peut être préférable pour le client d'en avoir connaissance, car elle peut générer des contraintes de choix de solutions et d'implantation.

Il faut entendre ici par le terme plateforme, l'environnement de virtualisation (mode IaaS) ou celui d'accueil des applications (mode PaaS). Une entité est une machine virtuelle ou une application.

Par définition, une plateforme doit offrir, à l'entité qui l'utilise, des services complètement indépendants de la localisation et de la présence concurrente d'autres entités utilisatrices. La plateforme est non seulement virtuelle, mais elle devient une chose qui présente un niveau d'abstraction plus fort que celui qu'on lui connaissait dans une configuration *on-premices* ou hébergée sur des moyens dédiés.

Prenons l'exemple du stockage sur Windows Azure. Il n'est jamais fait référence à un système de stockage physique, ni à un système de gestion de fichiers classique. On utilise des bases de données, des BLOB (Binary Large Object) destinées à des accès directs aux données, des *streams* (flux de données) destinés à être traités séquentiellement du début à la fin.

Encore une fois, la migration vers le cloud n'est pas un simple portage. Elle nécessite de reconsidérer l'architecture des solutions informatiques.

Remarque corollaire : la définition d'une solution *cloud* en mode PaaS n'est possible que pour des éditeurs de systèmes d'exploitation ou d'environnement de fonctionnement d'applications : par exemple Microsoft avec Windows Azure et .Net, IBM avec Websphere, Oracle avec son SGBD et Java. Le logiciel libre n'est pas en reste avec des initiatives telles qu'Open Cloud et CloudStack.

Impacts sur le réseau.

Les ressources de service d'une solution *cloud* sont situées en dehors de l'entreprise. Il est donc fondamental que le réseau qui permet de les utiliser soit l'objet de toutes les attentions.

Disponibilité

Il faudra chercher une haute disponibilité du réseau. Des dispositions doivent être prises pour réparer au plus vite en cas de défaillance : engagement contractuels de disponibilité, contrats de maintenance, pièces de rechange… Si besoin est, les chemins entre le client, dans l'entreprise ou sur Internet, doivent être réellement multiples. Il est recommandé de se pencher sur les aspects techniques des prestations fournies par les opérateurs de télécommunication.

Performances

D'autre part, les performances d'Internet ne sont pas celles d'un réseau local. Les applications implantées dans le *cloud* doivent être conçues pour offrir leur qualité de service en utilisant la performance disponible sur un réseau étendu. Cet objectif est aujourd'hui atteint lorsque les applications sont architecturées pour être accessibles par un navigateur Web ou un client léger.

Protection

Le réseau d'une entreprise est traditionnellement protégé de façon périphérique. Un ou plusieurs firewalls protègent la frontière entre Internet et le réseau interne. Cet équipement dispose de filtres qui agissent aussi bien au niveau des flux réseau qu'applicatifs.

Avec le *cloud*, le réseau de l'entreprise et Internet, qui permet d'accéder aux services du *cloud*, ne font logiquement qu'un. Par nature, les chemins utilisés ne peuvent pas être identifiés.

Le modèle fondé sur une protection périphérique devient obsolète. Le nouveau modèle qui prévaut considère les connexions d'application à application. Tous les équipements, serveurs et postes de travail, disposent de leurs propres fonctions de protection d'accès au réseau. Chacun d'entre eux est paramétré pour faire confiance à ses partenaires applicatifs identifiés, à l'exclusion de tout le reste.

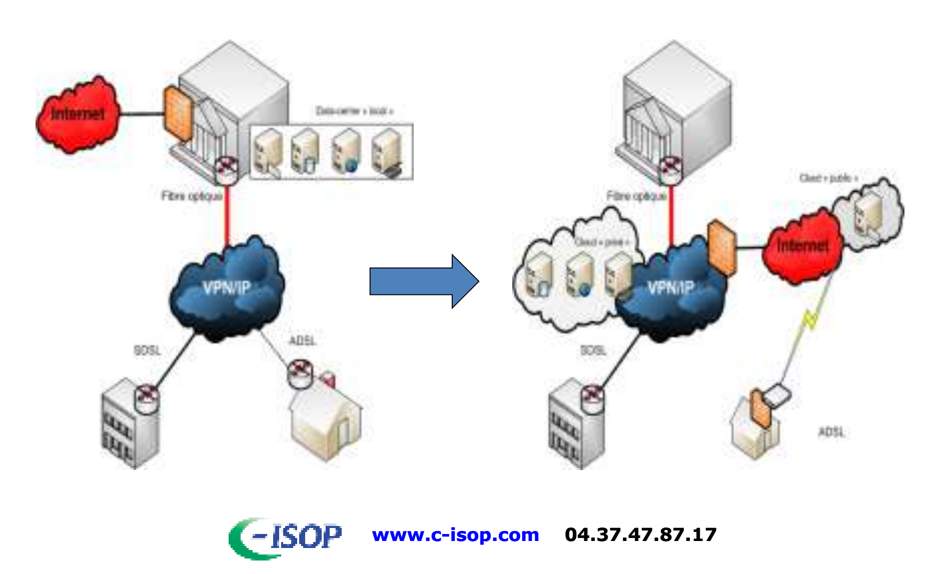
Les technologies mises en œuvre sont les suivantes :

- recommandations du Jericho Forum®, « dé-périmètrisation » du réseau,
- IPsec, SSL,
- Public Key Infrastructure (PKI),
- Microsoft Direct Access et Network Access Protection (NAP),
- Cisco Virtual Office…

Capacité

Il peut être nécessaire d'augmenter la capacité de l'accès à Internet afin de disposer de la bande passante nécessaire au bon fonctionnement des applications. Dans le cas d'organisations multi-sites, cela peut conduire à remettre en cause la centralisation des flux vers le data center interne au profit d'un accès directement au travers du VPN IP de l'Entreprise.

Cloud Computing



La gestion d'identité

L'adoption d'une solution *cloud computing* dans l'infrastructure informatique d'une entreprise est réalisée concurremment à l'exploitation d'une infrastructure privée. En principe, les identités sont déjà gérées dans cette infrastructure existante. Comment étendre cette gestion dans le *cloud* ?

L'annuaire privé est la référence

Le *cloud* accède à l'annuaire privé pour authentifier ses utilisateurs. Il est nécessaire de construire un accès sécurisé du *cloud* sur l'annuaire privé : authentification mutuelle des deux parties prenantes, *cloud* et annuaire privé, chiffrement des données sur les réseaux. Il s'agit d'un cas spécifique d'utilisation du protocole LDAP.

L'annuaire privé de l'entreprise et celui du *cloud* sont synchronisés

Ils sont synchronisés à intervalle de temps régulier.

La synchronisation des mots de passe peut s'avérer source de failles dans le système de sécurité s'ils doivent être stockés de façon à pourvoir être lus « en clair ». La solution consiste à disposer d'un algorithme de chiffrement commun entre l'annuaire privé et celui du *cloud*.

Dans ce cas d'utilisation, il faut aussi traiter les cas de divergence entre le contenu de chacun des deux annuaires, donc prévoir des mécanismes de réconciliation.

L'annuaire dans le *cloud* devient la référence

L'entreprise utilisatrice fait le choix d'implanter le service d'authentification des utilisateurs sur le *cloud*, typiquement en mode SaaS. Ce choix est guidé par l'évaluation de tous les critères que nous évoquons dans ce livre blanc, et d'autres. De tels services existent : Microsoft Live ID, Open ID (notamment avec une solution Verisign), Google et Facebook (avec des contraintes sur la mise dans le domaine public des données des utilisateurs).

En règle générale, les mécanismes proposés sont ceux des identités fédérées exposés ci-dessous.

Identités fédérées

L'architecture est fondée sur des mécanismes de fédération d'identité. Les annuaires sont multiples. Ils gèrent les identités et/ou les droits d'accès des utilisateurs. Quant à elles, les applications sont de type *claim based* : elles réclament, aux mécanismes de fédération d'identité, des données à propos des utilisateurs.

La mise en œuvre d'une fédération d'identités consiste dans des accords d'approbation qui sont passés entre les parties prenantes, *cloud*, entreprise et tiers (clients, fournisseurs, partenaires). Ces accords sont matérialisés par des certificats qui permettent

- l'authentification mutuelle des parties prenantes,
- la signature de jetons contenant les informations d'identité et de profil des utilisateurs.

Cette dernière solution présente les avantages

- de permettre de gérer séparément les problématiques d'identification, d'authentification, de rôle et de données personnelles associées à chaque utilisateur,
- de permettre des architectures, de la plus simple à la plus complexe, dans le domaine de la gestion d'identités et de l'accès aux applications.

Elle constitue l'état de l'art. Ces mécanismes sont normalisés (OASIS, SAML, projet Liberty Alliance) et implantés dans par bon nombre d'éditeurs : Entrust, IBM, Microsoft, Novell, Ping Identity, SAP et Siemens.

L'autorisation des accès

Ce chapitre n'a traité que de la gestion des identités, proprement dites, c'est-à-dire l'existence des utilisateurs humains et la gestion de leur authentification. Pour autant, l'accès aux ressources applicatives par ces utilisateurs n'est pas encore évoqué.

D'une façon générale, l'état de l'art recommande que l'accès aux ressources des applications (fonctions, données) soient fondé sur les rôles des utilisateurs. Cela allège les mécanismes de gestion. Cette recommandation n'est pas spécifique au *cloud*.

Les processus de provisionnement et de dé provisionnement doivent intégrer tant les applications internes à l'entreprise que celles hébergées dans le *cloud*. Ce dernier point nécessite la création ou l'adaptation de l'organisation (processus) et de l'outillage.

Localisation des données hors de l'entreprise

Vie privée

Naturellement, le cloud computing est soumis à l'observation des règles classiques liées à la protection de la vie privée en France et en Europe.

Notamment, la Directive 1995/46/EC encadre le traitement et l'export de ces données en obligeant les parties prenantes à justifier ce traitement, à en notifier les autorités nationales - en France, la CNIL - et les individus concernés, et à entourer ces manipulations des protections techniques jugées nécessaires.

Point important : cette réglementation restreint également l'export des données personnelles vers des pays étrangers à l'UE. Ces délocalisations ne sont en effet tolérées que vers les pays offrant des "protections adéquates". Il est à noter que les USA, principaux fournisseurs de solution de cloud computing, ne font pas partie de cette liste, mais bénéficie cependant des largesses prévues par le mécanisme Safe Harbor. Dans ce cas particulier, les données peuvent donc être exportées vers les USA, sans qu'un traitement ultérieur soit pour autant autorisé.

Toute entreprise manipulant des données personnelles au travers de solutions de cloud computing doit donc porter une attention particulière aux garanties offertes par leur fournisseur en terme de sécurité, de traitement et d'export physique des informations ainsi collectées.

Données confidentielles

Pour les données ne relevant pas de la sphère personnelle, peu de réglementations existent en dehors de celles prévues dans le cadre spécifique de la défense.

Mais il en est une qui, bien qu'américaine, perturbe particulièrement les entreprises du monde entier, USA exceptés.

Le "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism act" - autrement appelé "USA PATRIOT ACT" - pose en effet des problèmes de confidentialité graves pour les données de toute nature.

Adopté dans la foulée des attentats de 2001, cette législation court jusqu'en 2015. Elle autorise les perquisitions secrètes, hors contrôle d'un juge, par les autorités américaines, de toute donnée stockées par :

- Une entreprise de droit américain (e.g. Google, Amazon, Microsoft, Apple, HP, DropBox, etc.), ainsi que leurs filiales dans le monde, quelle que soit la localisation effective de cette donnée (i.e. même si cette donnée est physiquement stockée en Europe)

- Un serveur hébergé sur le sol américain, quelle que soit la nationalité de l'entreprise qui l'exploite.

En d'autres termes, aucune donnée stockée sur un service de cloud américain ne saurait, aujourd'hui, être considéré comme confidentielle. Ce constat est l'une des principales justification à l'émergence de solutions de stockage cloud nationales et de confiance, notamment en Allemagne et en France.

Toute entreprise "sensible" ou manipulant des données confidentielles (R&D, données stratégiques, secrets commerciaux ou financiers, etc.) doit bien cerner ce risque avant de décider d'utiliser des services de cloud computing étrangers.

Ce qu'il faut retenir…

Impact sur les applications	Impact sur le réseau	Impact sur la gestion d'identité et la localisation des données
- Les applications Saas sont paramétrables et adaptables aux différentes solutions clients grâce à des connecteurs dédiés, proposés par les éditeurs - Certains éditeurs ouvrent leur plate-forme à des partenaires (*à travers des API)*, pour développer et proposer des extensions et modules complémentaires - Mises à jour transparentes pour les utilisateurs - Fluidité en termes d'utilisation - Mode "hors connexion" proposée par la plupart des éditeurs - Facilite la mobilité des équipes - Sécurité maximale en cas de perte ou de vol, si le modèle est de type "client léger" et qu'il n'y a pas de données stockées en local sur le poste	-Transfert de charge du réseau interne vers l'Internet, ce qui peut générer des goulots d'étranglement - Optimisation du réseau / réduction de bande passante : → technologies standard du Web type XML → optimisations des interfaces → moins de téléchargements (*grâce aux navigateurs html et culture du lien plutôt que des pièces jointes)* → accès via le Net depuis un mobile → blocage de spams/virus à l'entrée sur l'email → En général, seules des trames d'affichage transitent sur le réseau *(accès aux données des applications SaaS via un navigateur)* *- Toutefois, il peut exister des application Saas Client serveur* *D'autre part, le réseau peut être sollicité en mode saturation lors du chargement initial des données* - Pas de système d'exploitation - Adaptabilité à tout type de navigateur Internet et de matériels - Disponibilité 24h/24h chez la plupart des fournisseurs de services	- Haut niveau de sécurité des fournisseurs de service sur l'accès aux données hébergées, en raison des mécanismes d'authentification. - Possibilité de renforcer ces mécanismes par des solutions mises en place, dans l'entreprise, de gestion d'identités *(placées en amont d'un lien unique avec le fournisseur de solutions Cloud)* - Pour la synchronisation avec l'annuaire LDAP, le processus est le même que lors de l'installation d'une solution "On premise" *(à condition que l'éditeur propose les connecteurs dédiés)* - Un outil SSO est indispensable dans ce cadre, afin de réaliser une synchronisation régulière pour faire lien entre l'application de l'entreprise et le fournisseur de service - Sauf demande expresse, les données ne sont plus localisées géographiquement. S'assurer de la compatibilité de cet état de fait avec la nature des données stockées et la réglementation qui s'y rattache

La sécurité.

L'utilisation d'applications Cloud a un impact important sur la sécurité. En effet les technologies de la sécurité, aujourd'hui bien établies (Firewall, VPN, VPN-SSL, etc.), sont aussi bousculées par les nouveaux usages associés à ces nouvelles applications. Cependant les concepts de base restent les mêmes.

De manière générale, la mise en place d'application Cloud permet aux services informatiques de l'entreprise (SI et SSI) de repenser le schéma de sécurité et d'appréhender les nouvelles problématiques :

- La confidentialité de la donnée, localisée hors de l'entreprise
- Le transport de la donnée vers le terminal de l'utilisateur
- La sécurité du terminal de l'utilisateur
- L'authentification de l'utilisateur

La confidentialité de la donnée

Lors de la mise en place d'une application Cloud, un des impacts majeur sur la sécurité est la localisation de la donnée hors de l'entreprise. Cette localisation hors les murs fait peser un risque physique sur celle-ci. Il existe plusieurs solutions pour lever ce risque.

La première est la maitrise de l'environnement de la solution Cloud, et en particulier son hébergement. Cela suppose un lien très fort avec le fournisseur d'application qui impose contractuellement une localisation de donnée, et un niveau de sécurité physique associé. Cette solution a un coût important et son approche ressemble plus à de l'hébergement qu'a une solution d'application Cloud.

La deuxième solution consiste au chiffrement de la donnée afin d'en assurer la confidentialité. Ce chiffrement peut être intégré complètement à l'application Cloud, ou assuré par un mécanisme externe à cette application. Dans ces deux cas, le chiffrement de la donnée doit être proposé par le fournisseur d'application et intégré au service. Le cout de cette solution est important, en termes financier, mais aussi en performances sur l'application. En effet, le chiffrement systématique des données peut avoir un impact sur la performance générale de l'application.

Ce qu'il faut retenir

La confidentialité des données, associée à la localisation de celles-ci, est un élément important de la sécurité des applications Cloud, en termes de couts et de performances. Il faut donc se poser la question au début du projet : « quelles sont mes données assez sensibles pour que je doive investir dans leur confidentialité ? ».

Transport des données

Le transport des données est le second problème des applications Cloud : si la donnée est en sécurité dans le Datacenter (quelle que soit la méthode), il faut qu'elle le soit aussi pendant son transport jusqu'au terminal de l'utilisateur.

La plupart du temps, les données transitent sur un réseau non sécurisé tel qu'Internet.

Le risque principal dans ce cas est l'écoute sur le réseau à des fins d'espionnage. Pour lever ce risque, la seule solution est le chiffrement des communications entre l'application Cloud et le terminal de l'utilisateur.

Deux solutions techniques sont envisageables.

La première consiste à utiliser un tunnel VPN (de type IPsec) permettant d'assurer le chiffrement et l'authentification des données transitant sur le réseau, entre un concentrateur VPN devant le serveur hébergeant l'application Cloud et le terminal de l'utilisateur. Cette solution a pour avantage d'être extrêmement sécurisée. Elle a par contre l'inconvénient d'être lourde à mettre en place, tant au niveau de l'infrastructure Cloud qu'au niveau de l'utilisateur. Les technologies VPN IPSec sont, de plus, difficilement interopérables et sont donc contraires au principe de souplesse et de simplicité des applications Cloud.

La seconde solution consiste à utiliser les technologies SSL pour chiffrer et authentifier les données transitant sur le réseau. Cette solution a pour avantage d'être très simple à déployer et très interopérable. De plus, elle possède un niveau de sécurité élevé. Elle a comme inconvénient d'être très fortement liée à l'application, et oblige donc le fournisseur d'application Cloud à prendre en compte cette contrainte au moment du développement de son application. La plupart des développeurs d'applications Cloud prennent en compte cette technologie et la propose en standard dans celles-ci.

Ce qu'il faut retenir

La confidentialité des données lors de leur transport est un élément à prendre en compte afin d'éviter des fuites d'informations, très aisées à récolter sur les réseaux non sur (Internet). Avec les technologies SSL, très largement déployées par les développeurs d'applications, la mise en place du chiffrement est assez simple et peu coûteuse.

La sécurité du terminal de l'utilisateur

La sécurité du terminal de l'utilisateur est l'aspect le plus difficilement appréhendable. En effet, la sécurité du terminal n'est pas directement liée à l'approche Cloud, mais elle peut directement impacter la sécurité de l'application Cloud, surtout avec la démocratisation du BYOD (Bring Your Own Device), facilitée par les applications Cloud.

La sécurité du poste de travail de l'utilisateur, moins maitrisée et plus nomade, devient donc un enjeu important car ce poste est directement connecté à l'application Cloud : il en est une porte d'entrée. Le risque principal est l'introduction d'un attaquant sur le réseau de l'application Cloud à des fins malicieuses, via le poste de travail de l'utilisateur.

La solution technique pour lever ces risques d'attaques n'est pas « unique » et dépend du type de terminal utilisé.

La première solution est l'utilisation de logiciels de sécurisation du poste de travail. Ils intègrent souvent :

- Un antivirus
- Des contrôles de ports USB
- Des contrôles des connexions sans fil
- Des contrôles des applications locales

Des produits complets existent sur le marché pour les PC et permettent d'avoir un niveau de sécurité très élevé. Malheureusement il existe très peu de solutions pour les terminaux mobiles, ou alors très partielles (les solutions MDM proposées par les opérateurs sont plutôt émergentes).

La seconde solution est l'éducation des utilisateurs. Un certain nombre de bonnes pratiques et d'usages « sages » permettent d'éviter dans la plupart des cas un certain nombre d'attaques. Cependant, c'est une solution très partielle qui n'apporte pas un niveau de sécurité acceptable. Elle est à combiner avec au moins un logiciel d'Anti-Virus/Anti-Spyware afin d'assurer le minimum de sécurité.

Ce qu'il faut retenir :

La sécurité du terminal impacte directement la sécurité de l'application Cloud.

Les solutions de sécurisation du poste de travail (antivirus évolués pour PC) sont très fortement préconisées pour l'utilisation du Cloud, mais cette recommandation n'est pas spécifique au Cloud et s'appliquent de façon général pour l'usage du SI de l'entreprise.

Le Cloud, en autorisant une plus large gamme de terminaux, notamment smart phones et tablettes avec différents OS, peut toutefois complexifier la généralisation de ces solutions de protection.

L'éducation des utilisateurs par des « chartes » est une approche complémentaire à la mise en œuvre de ces outils.

Ce qu'il faut retenir :

Nous avons parcouru dans ces paragraphes les différentes problématiques et les moyens techniques pour y répondre.

La solution monolithique n'existe pas, mais dans la grande majorité des cas, l'intégration de la sécurité dans l'application Cloud permet d'avoir un rapport « sécurité/cout » optimal. La mise en place de ces solutions à un cout non négligeable, mais elle est impérative pour assurer la sécurité des données sensibles de l'entreprise dans sur ses applications Cloud.

Cependant, la mise en place de celles-ci reste une opportunité pour les SI et SSI de remettre en cohérence leur architecture de sécurité, souvent élaborée au fil du temps.

Normes

Si le *cloud* doit consister à apporter les services informatiques dans les entreprises aussi simplement que l'électricité de la part de l'EDF, il serait normal de comparer la standardisation du Cloud avec la standardisation qui existe à propos de la tension et de la puissance délivrés au niveau d'une prise de courant.

Force est de constater qu'il n'existe aucune norme spécifique à propos des services fournis par le *cloud*. Il existe cependant tout ce qui concerne l'informatique, en général, au niveau technique (Web, réseaux, systèmes, bases de données…) et au niveau des systèmes de gestion (qualité, sécurité, pratiques d'exploitation…).

La Chine et la Corée du Sud ont aujourd'hui quelques velléités pour avancer rapidement sur le terrain de la normalisation pour chercher à s'imposer dans la fourniture de services. En Europe, l'AFNOR, entre autres, cherche des contributeurs pour contrer cette initiative perçue comme hégémonique. L'objectif est de proposer des normes stables à partir de 2014. Vraisemblablement un rêve dans un monde où les acteurs, sur des architectures propriétaires, cherchent à rentabiliser des investissements qui se comptent en milliards de dollars.

Ce qu'il faut en retenir :

L'implantation d'une ou plusieurs applications dans le *cloud* ne peut se résumer à un simple portage technique.

Cela pouvait être le cas dans une solution d'infogérance dans laquelle le client conservait la maîtrise de l'architecture.

Cela ne l'est plus dans le *cloud* où l'infrastructure est virtualisée et abstraite.

Il faut reconsidérer architecture, implantation et sécurité, dans un environnement qui est loin d'être stable.

Comment mettre en œuvre le *cloud computing* ?

Les études en amont du projet Cloud Computing

La phase d'étude en amont d'un projet Cloud prend une importance accrue en regard d'un projet classique (interne). Il est bon en effet de faire un point sur l'existant avant de définir la cible et par quel chemin on désire l'atteindre.

Sa mise en œuvre peut se décliner en **6 phases**.

1. Elaboration de la roadmap

- Consolidation de l'existant, virtualisation …
- Les priorités et objectifs (Existant, nouveaux besoins, nouvelles applis …)
- Usages métiers concernés
- volet sécurité, confidentialité, juridique importants par rapport à un projet classique
- évolution de l'organisation

2. Etablir une sélection des services dont le fonctionnement est adapté au mode Cloud

Certains services sont plus adaptés à l'informatique en nuage que d'autres (exemple : messagerie, bureautique). C'est pourquoi il est essentiel de bien les hiérarchiser.

Critères de choix :

- Exigences de la plateforme matérielle et logicielle,
- Complexité et criticité des applications métier
- Sécurité et sensibilité des données…

3. Conception de l'architecture Cloud

Quatre questions à se poser pour définir l'architecture sur laquelle s'appuiera le modèle de nuage.

- Quels services veut-on fournir ?
- Quel mode de gestion ?
- Comment les utilisateurs vont-ils accéder à ces services ?
- Quel niveau de service ?

4. Choix du modèle de nuage

En fonction des services éligibles au Cloud le modèle de ce dernier sera public ou privé:

- Public pour les services présentant peu de risque comme les applications d'échange et de collaboration, les services d'assistance …
- Privé pour les entrepôts de données, les applications métiers …

(On disposera les environnements de test sur l'un ou l'autre)

5. Estimation du retour sur investissement

Quelles sont les économies réalisées par l'implémentation d'un Cloud ?

- Sur l'infrastructure
- Sur l'immobilier
- Sur les consommations
- Sur la gestion, l'administration
- Sur les RH

6. Mise en œuvre de la stratégie, de la roadmap et des services Cloud

Après la première phase consistant à automatiser et virtualiser l'infrastructure, il est judicieux de lancer un projet pilote sur un périmètre restreint et dont on a analysé la mise en œuvre en mode « Cloud computing », pour permettre aux équipes SI ainsi qu'aux utilisateurs de se familiariser avec ce concept pour ensuite le déployer progressivement, couche par couche.

Ce processus peut avoir également l'avantage de démontrer aux financiers l'intérêt de la solution.

La Conduite du changement

- **COMMUNIQUER**

  Il est nécessaire de mettre en place une communication transverse, adaptée à chaque population. La diffusion des informations est réalisée avec l'appui d'un **sponsor** interne, visible, reconnu et présent tout au long du projet. Les premières informations à mettre en avant sont :

  POURQUOI LE CLOUD ? (raisons financières, réactivité, agilité, innovation, se recentrer sur son métier …).

  COMMENT va-t-on passer sur le Cloud ?

  QU'EST CE QUE CELA IMPLIQUE ?

  Pour les utilisateurs : Pour accompagner le changement, Information et formation des utilisateurs sont nécessaires y compris sur des applications triviales comme la messagerie. Ces informations doivent porter sur le changement dans la fourniture du service:

  - La gestion devient formelle.
  - L'utilisateur dispose d'un catalogue de service.
  - Le niveau d'organisation augmente. (Processus de validation des demandes)
  - Les appréhensions concernant la « lourdeur » d'un tel dispositif doivent être contrebalancées par plus d'efficacité et de flexibilité pour l'utilisateur.

  Pour le personnel DSI – impacts RH

  L'évolution des métiers et la transformation du rôle de la DSI sont au centre de la communication interne. Cette dernière doit mettre l'accent sur la valorisation des compétences par son utilisation sur les projets technologiques de l'entreprise.

- **MOBILISER**

  Les utilisateurs motivés et convaincus doivent servir de « têtes de pont » pour convaincre et motiver les esprits sceptiques. Des « Power Users » seront désignés pour porter le projet sur le terrain. La création de maquettes pourra impliquer les utilisateurs dans la réflexion et les familiariser avec les changements annoncés. *Mobiliser durablement les utilisateurs c'est avant tout les impliquer dès le début du projet, les faisant participer activement à sa construction.*



- **FORMER**

  Les formations seront adaptées aux populations en fonction des services qu'elles sont en droit d'attendre.

- **SUPPORTER**

  Pendant le déploiement et pendant une durée (à déterminer selon le projet) « post-déploiement » il est judicieux de créer une cellule support dédiée. Dès la mise en production du projet et sur toute la période définie de mise en observation, l'utilisateur ne doit pas se sentir livré à lui-même. Il doit bénéficier de l'écoute active du support. N'oublions pas que dans certains cas il peut s'agir d'une véritable révolution dans les méthodes de travail.

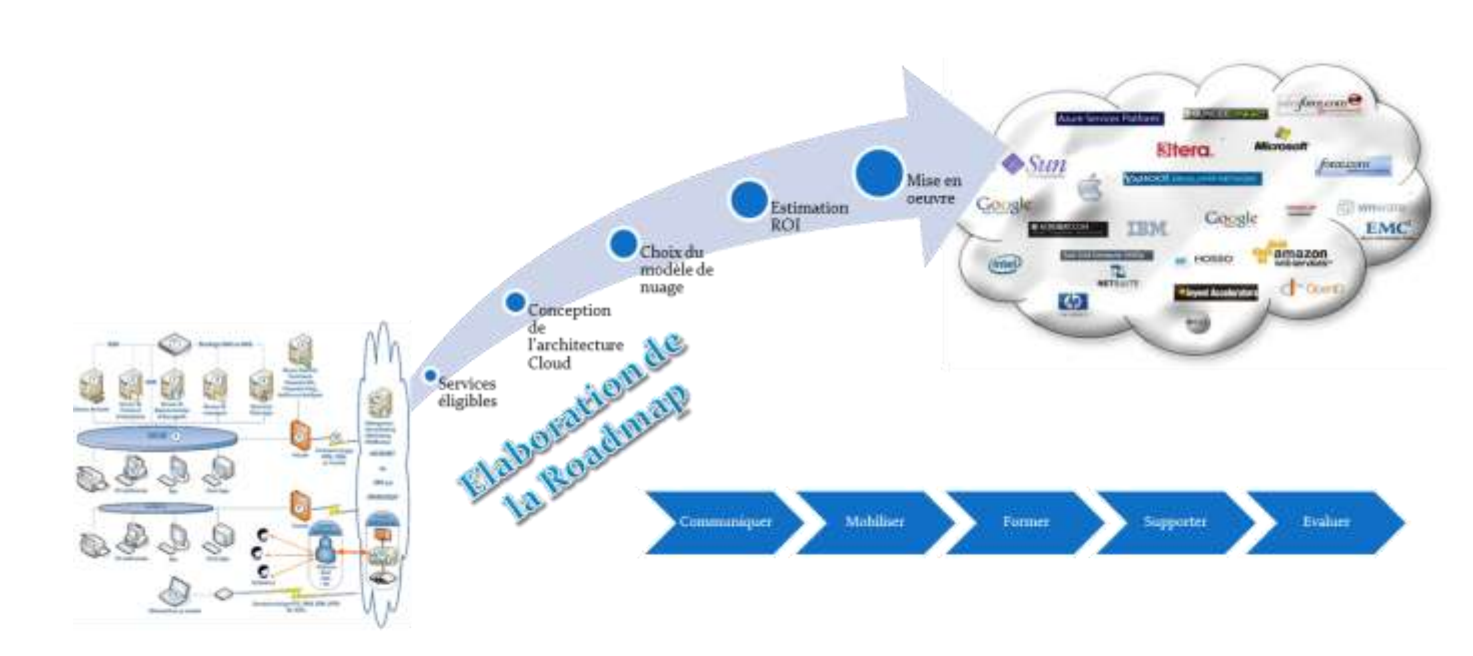
  Pour les plus autonomes la mise à disposition des documents de formation (intranet) ainsi que de procédures simples peut être une solution.

- **EVALUER**

  Avant, pendant et après un projet Cloud, l'évaluation des trois paramètres suivants est un gage de succès :

  - ✓ **Au début du projet :** Niveau de préparation des utilisateurs au changement,
  - ✓ **Pendant le projet :** Bon déroulement des formations utilisateurs
  - ✓ **A la fin et après le projet :** Evaluer les apports et la cohérence avec ce qui a été annoncé. Communiquer les résultats.

Etude en amont et conduite du changement



Ce qu'il faut retenir …

Un projet Cloud se distingue avant tout d'un projet informatique classique par la prédominance de la partie étude en amont du projet et l'importance de la conduite du changement.

Pour le projet proprement dit, les méthodes de gestion de projet classiques restent valables.

On ne parle presque plus technique lors d'un projet Cloud. Il s'agit d'un jeu de construction où toutes les pièces ont besoin de données en entrée (ou pas !) et fournissent des services en sortie.

Ces services peuvent être directement utilisables par le client final (bureautique par exemple) ou à destination d'autres parties du SI qui utiliseront ces services en entrée pour en fournir d'autres en sortie (EDI par exemple).

Dans ce type de projet on va donc reporter les efforts sur la partie « construction » de la solution et sur le côté organisation des différentes briques.

Sur le plan de la conduite du changement on dira sans surprise qu'encore une fois la COMMUNICATION sera au cœur de la réussite d'un projet Cloud avec la FORMATION car nous touchons là des changements profonds dans l'organisation des DSI.

Côté utilisateur final, le changement dans la façon de travailler devrait être moins important. Les efforts à mener étant sur le ressenti des performances.

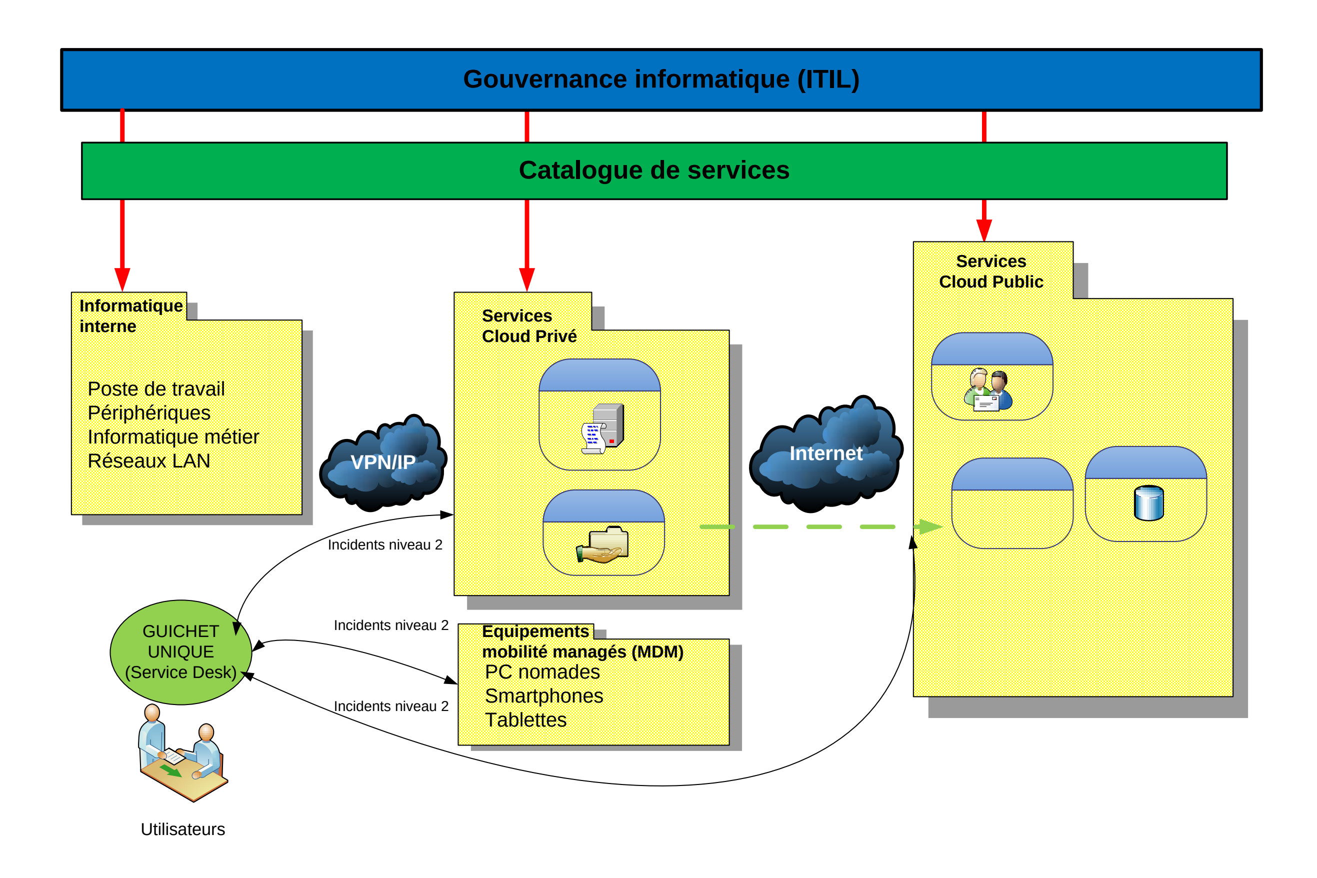
Favoriser le changement par une information au plus près pour éviter les résistances, les oppositions.

L'exploitation d'une solution *cloud*

L'exploitation d'une solution de Cloud Computing doit s'intégrer au sein des procédures et processus d'exploitation déjà en vigueur au sein de l'entreprise.

Si l'entreprise se conforme à des bonnes pratiques de gouvernance du SI tels que par exemple ITIL, ce référentiel doit explicitement être mentionné dans les marchés et contrats des solutions Cloud et il doit être exigé à minima du prestataire qu'il fournisse les interfaces, processus et traçabilités permettant au service desk de l'entreprise de gérer les demandes utilisateurs, les incidents, les problèmes, les changements, etc…

Les différentes briques de Cloud Computing, publics ou privés, doivent s'intégrer au sein du catalogue de services de l'entreprise de façon à offrir aux instances de gouvernance du SI une vision homogène du SI, indépendamment de la stratégie Cloud Computing adoptée.



Contrats, SLA

En dehors de ces exigences générales de conformité à l'organisation et aux processus de l'entreprise, les points spécifiques de vigilance propres au Cloud Computing sont :

- ✓ La localisation géographique des données et des traitements, qui doivent être compatibles avec les exigences réglementaires s'appliquant à l'entreprise (CNIL, …).
- ✓ La mise en œuvre de processus d'archivage permettant la réversibilité en cas de défaillance du prestataire

- ✓ Les outils et moyens de mesure de la performance applicative, de bout en bout, tels que les sondes, robots de tests et les processus de diagnostic et réparation en cas de dégradation des performances, avec les SLas et pénalités associées
- ✓ Les engagements de disponibilité de la solution, les Slas associés et les outils de l'entreprise permettant de superviser celle-ci
- ✓ Les modalités d'évolution des versions permettant une information suffisamment en amont du service desk pour assurer la conduite du changement et les formations éventuelles des utilisateurs
- ✓ Les reporting associés au Slas

Gestion de la transition et réversibilité

Les prestations et services devant être assurées par le prestataire pour participer au processus de migration et de peuplement des bases de données doivent être détaillés précisément.

L'archivage des données doit être indépendant du prestataire (et si possible interne), afin de pouvoir assurer une réversibilité même si la société se trouve brusquement défaillante.

La clause de réversibilité du contrat doit détailler précisément les livrables attendus de la part du prestataire pour assurer le transfert soit en interne, soit vers un autre prestataire Cloud.

Ce qu'il faut retenir :

L'exploitation d'une solution Cloud Computing doit s'intégrer dans l'organisation et les processus globaux de la gouvernance informatique de l'entreprise.

Les briques Cloud doivent être décrites au sein du catalogue de services.

Une attention spécifique doit être apportée dans la rédaction des contrats sur des points tels que la localisation et l'archivage des données, le contrôle des performances et de la disponibilité, le processus de migration initiale, la gestion des changements en cours de contrat et la réversibilité.

Conclusions

Si, comme Pierre, vous vous interrogez sur l'opportunité de gérer l'un des projets informatiques au moyen d'une solution Cloud Computing, nous espérons que ce livre blanc pourra vous aider à prendre la bonne décision.

Et, à défaut d'apporter toutes les réponses dans un domaine complexe en pleine mutation, au moins vous lister les bonnes questions et vous encourager à expérimenter les apports du Cloud Computing dans le cadre d'une expérience pilote.

Pour en partager prochainement le retour d'expérience avec nous…

